INTEGRANTES
Anderson Barragan ⟹ 201719821
Sebastian Mujica ⟹ 201633171

Análisis del problema

Datos y riesgos

Vemos, según la descripción del caso, los elementos con los cuales interactúan los clientes y el portal web (por el contexto asumimos Colpensiones). Vemos la posibilidad de acceder a datos sensibles de los afiliados con las credenciales que ingresan los usuarios a la entidad. Vemos a continuación en la descripción del prototipo el tipo de credenciales compartidas (cédula y contraseña) para la autenticación de los afiliados.

Dado que los datos compartidos que a fin de cuentas la información más sensible que viajará en el caso serán las credenciales de los clientes que quieren averiguar el estado de su cuenta. La importancia de estos datos es que si estos lograsen ser accedidos por personal no autorizado permitirían el acceso a información sensible (como su estado de cuenta) lo que conllevará a problemas a la institución (los evaluaremos más adelante).

La importancia de proteger estas credenciales se da por los posibles problema técnicos, legales y/o de privacidad que podrán surgir para la Colpensiones y sus afiliados.

Primero, con respecto a las credenciales de usuario; estas credenciales son las únicas que viajaran frente a la red externa al sistema interno de Colpensiones, por lo que solo analizaremos este lado. Con respecto a esta información, si fuese accedida (un man in the middle por ejemplo) podría (dado que los afiliados solo tienen accesos de lectura) poder obtener información sensible de los afiliados, no solo comprometiendo su seguridad y privacidad, sino que además, por el lado de Colpensiones, (posiblemente) rompiendo el contrato que se asume se estableció con los afiliados y la integridad y seguridad de los datos. Asumiendo un caso no mencionado por el contexto, pero presentado en el caso, la escritura por parte de los usuarios sería incluso más grave. En el caso de obtener permisos de escritura sobre la información contenida por Colpensiones, la información como los estados de cuenta, afiliados, deudas u otros podrían ser alterados ocasionando así que flujos de caja fueran modificados y generando pérdidas para Colpensiones al no tener una contabilidad correcta de sus elementos.

4 vulnerabilidades

A continuación, listas las cuatro vulnerabilidades encontradas en el sistema del portal web

1. *La primera vulnerabilidad está asociada con la integridad de los datos en la comunicación entre el cliente y el servidor web. Esto sucede debido a que un* `Man In The Middle` *podría aparecer en la comunicación entre el cliente y el servidor. Lo anterior, permitiría modificaciones en pasos importantes de la comunicación en tales mensajes como: Los algoritmos seleccionados por el cliente, lo que ocasionaría que el servidor le enviara «ERROR» como respuesta y la comunicación ser terminara, se reiniciara, o el cliente tuviera que enviar de nuevo el mensaje con los algoritmos. Además, esto ocasionaría otras vulnerabilidades que serán mencionadas más adelante.*

INTEGRANTES
Anderson Barragan ⟹ 201719821
Sebastian Mujica ⟹ 201633171

2. *La segunda vulnerabilidad está relacionada con la vulnerabilidad anterior, en la cual nuevamente un* `Man In The Middle` *estaría constante modificando los mensajes de confirmación del cliente y del servidor. Esto ocasionaría la denegación de servicios para el cliente, ya que la sesión se estaría reiniciando constantemente o terminando la sesión. Como consecuencia, el usuario nunca podría llegar al punto de autenticarse y obtener el valor que desea consultar.*
3. *La tercera vulnerabilidad está relacionada con* `DDoS`*, ya que el servidor no cuenta con protección ante ataques* `DDoS`*, se podrían realizar muchas peticiones provocadas por las conexiones de muchos usuarios en simultáneo a través de hilos. En estas peticiones, los usuarios podrían enviar siempre una confirmación de «ERROR» en el último mensaje, consiguiendo que la sesión se reinicie o se sobrecargue. De esta manera, el servidor finalmente comenzaría a denegar servicios, además sólo existe un servidor del portal web para atender las peticiones de los usuarios de todas las ciudades que desean acceder lo que agudiza la vulnerabilidad.*
4. *Al analizar la forma en la que son manejadas las credenciales de usuario en el sistema (dado que no se expone una forma diferente se asume así) posee dos vulnerabilidades:*
    a. *En primera instancia el almacenamiento de las credenciales aparenta ser realizado tanto en la base de datos principal de Colpensiones como en el* `backup` *de forma directa, es decir no se cifra, ocasionando así que si esta información fuese robada se obtendría en texto plano y con ella se podría acceder directamente al sistema dado que se obtendrían las credenciales.*
    b. *La segunda corresponde a la petición cuando ya se poseen las credenciales del cliente. Ya que la configuración del firewall del sistema permite bloquear direcciones con comportamientos o «extraños» dado que está «bien configurado», es posible que, como se mencionó en el literal inmediatamente anterior, si se obtienen las credenciales un atacante lograse bloquear las cuentas de los afiliados al realizar acciones no comunes para el sistema con estas credenciales.*